IN THE UNITED STATES PATENT
AND TRADEMARK OFFICE

Applicant(s): Zimmer et al.　　　　　)

Serial No.: 10/723,011　　　　　)

Filed: November 26, 2003　　　　　)

Assignee: Intel Corporation　　　　　)

For: Methods And Apparatus For Securely)
Configuring A Machine In A Pre-Operating)
System Environment　　　　　)
　　　　　)
Group Art Unit: Unknown　　　　　)
　　　　　)
Examiner: Unknown　　　　　)

)　I hereby certify that this paper is
)　being deposited with the United
)　States Postal Service with
)　sufficient postage as first class
)　mail in an envelope addressed to:
)　Commissioner for Patents, P.O.
)　Box 1450, Alexandria, VA 22313-
)　1450 on this date:

DATED: ___3/4/2004___

Mark C. Zimmerman
Registration No. 44,006
Attorney for Applicant(s)

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The patents and/or publications listed on the enclosed PTO Form-1449 are

submitted pursuant to 37 CFR §§ 1.56, 1.97, and 1.98. Copies of the patents or

publications are enclosed.

TIME OF FILING

This information disclosure statement is being filed to the best of the

undersigned's knowledge, before the mailing date of a first Office action on the merits. In

accordance with 37 CFR §1.97(b), no certification or fee is required.

METHOD OF PAYMENT

☒   No fee is required.

The Commissioner is authorized to charge any fee deficiency required by this paper, or credit any overpayment, to Deposit Account No. 50-2455. A copy of this paper is enclosed.

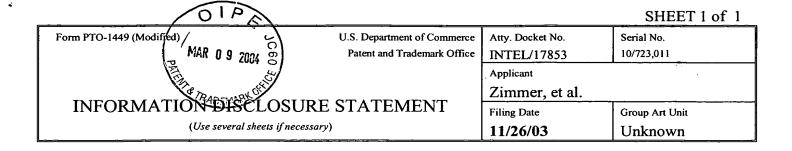Correspondence Address:

Respectfully submitted,

GROSSMAN & FLIGHT, LLC.
20 N. Wacker Drive
Suite 4220
Chicago, Illinois 60606
(312) 580-1020

DATED: 3/4/2004   By: _____

Mark C. Zimmerman
Registration No.: 44,006
Attorneys for Intel

Form PTO-1449 (Modified) /	U.S. Department of Commerce Patent and Trademark Office	Atty. Docket No. INTEL/17853	Serial No. 10/723,011
		Applicant Zimmer, et al.	
INFORMATION DISCLOSURE STATEMENT *(Use several sheets if necessary)*		Filing Date 11/26/03	Group Art Unit Unknown

		OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, etc.)
	C01	*What is BIOS? (Mini-FAQ)* [online], [retrieved on 09/29/2003]. Jupitermedia Corporation, 2003. Retrieved from the Internet <URL: http://www.sysopt.com/biosdef.html.
	C02	*What is Diffie-Hellman?* [online], [retrieved on 10/14/2003]. RSA Security Inc., 2003. Retrieved from the Internet <URL: http://www.rsasecurity.com/rsalabs/faq/3-6-1.html.
	C03	Symmetric-key Cryptography [online], [retrieved on 10/21/2003]. Jupitermedia Corporation, 2003. Retrieved from the Internet <URL: http://www.webopedia.com/TERM/S/symmetric_key_cryptography.html.
	C04	*TCPA Technical Overview for EFI.* Trusted Computing Platform Alliance, January 17, 2002. p.1-77.
	C05	Grawrock, D. *Trusted Computing Group Specifications.* Trusted Computing Group, April 17, 2003. p.1-13.
	C06	Grawrock, D. *Building the Trusted Client.* Intel Corporation, February 26, 2002. p. 1-22.
	C07	*Advanced Encryption Standard (AES).* November 26, 2001. p. 1.-47.

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance <u>and</u> not considered. Include copy of this form with next communication to applicant.